Lab-27: Configuring SIEM for GreenBloom Security Operations

Tatiana Meneses

February 17th, 2025

Overview

GreenBloom has been expanding its cybersecurity operations, and the executive team has prioritized improving threat detection capabilities. To achieve this, your team has been tasked with deploying and configuring a Security Information and Event Management (SIEM) solution using Elastic Stack. This will allow GreenBloom to centralize security logs, analyze threats in real time, and enhance its incident response capabilities.

Objectives

This lab will guide you through detecting and analyzing a simulated cyber attack using Elastic Security (SIEM). You will follow the Cyber Kill Chain attack phases, track malicious activity in Kibana, and create a detection and response report.

You will configure **Winlogbeat** to collect and analyze Windows event logs using an existing Elastic. You will install and configure Winlogbeat on a Windows 10 machine to monitor failed login attempts.

This exercise will help you understand how to integrate Windows event logs into an Elastic-based SIEM solution for security monitoring.

Your objective in this lab is to:

1. **Set up and configure Elastic SIEM** to collect and analyze security logs from GreenBloom's environment.
2. **Validate SIEM functionality** by executing **Atomic Red Team tests**—simulated attack techniques designed to test detection effectiveness.

Requirements

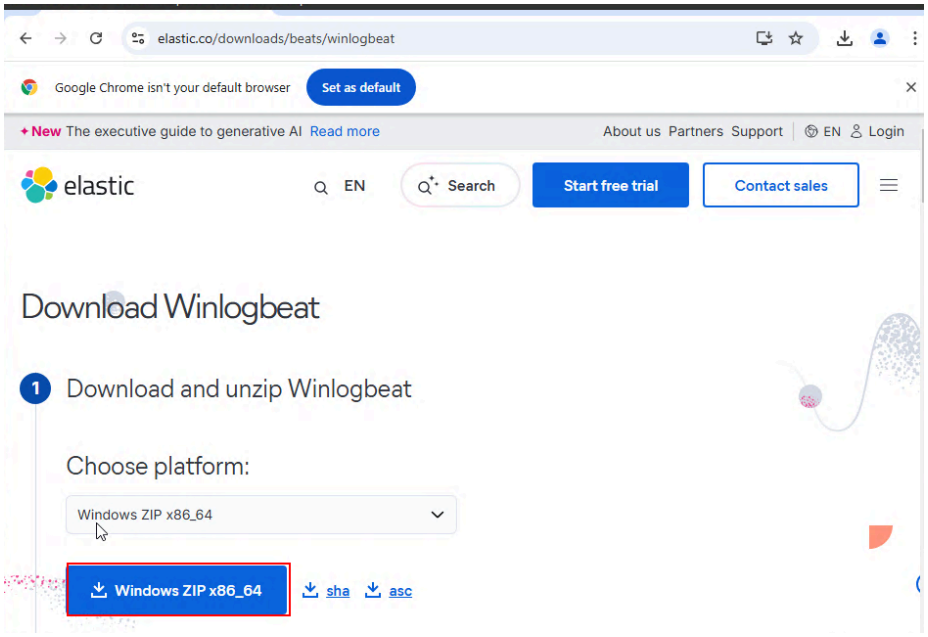
A virtualized environment with Ubuntu and Windows 10 VMs

Pre-installed and running Elastic

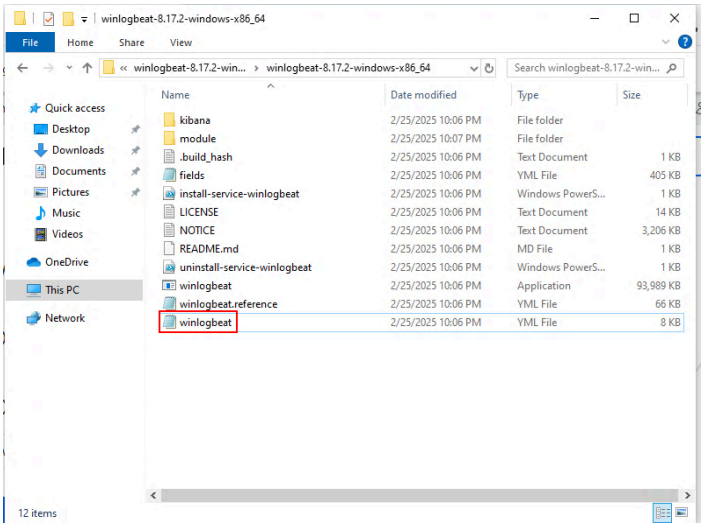
Network configuration set to NAT Network or Bridge Adapter

Part 1: Configure Winlogbeat

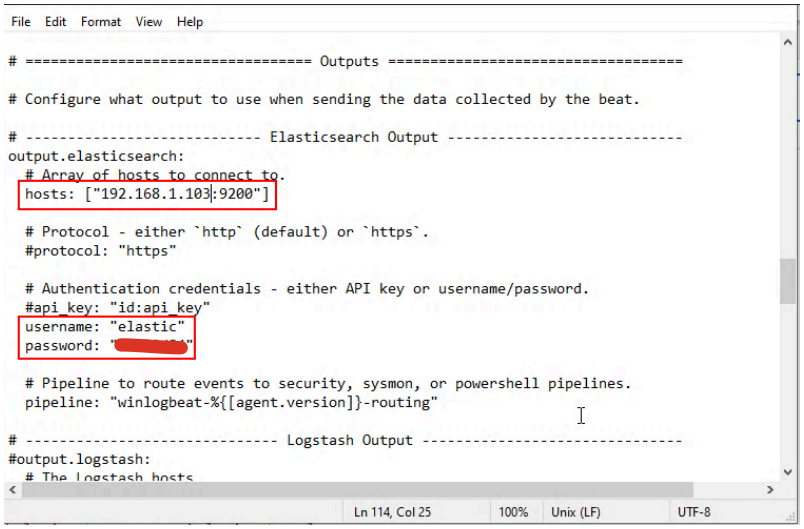
Download Winlogbeat: https://www.elastic.co/downloads/beats/winlogbeat



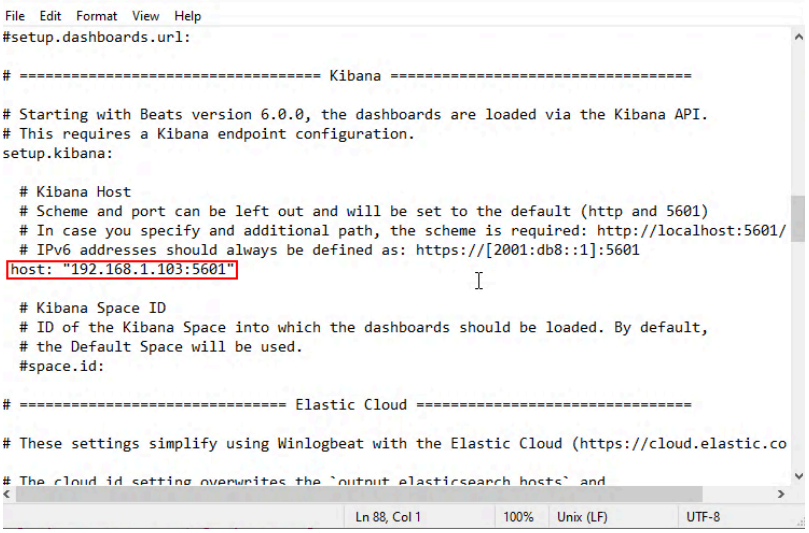
Edit winlogbeat.yml before installation:



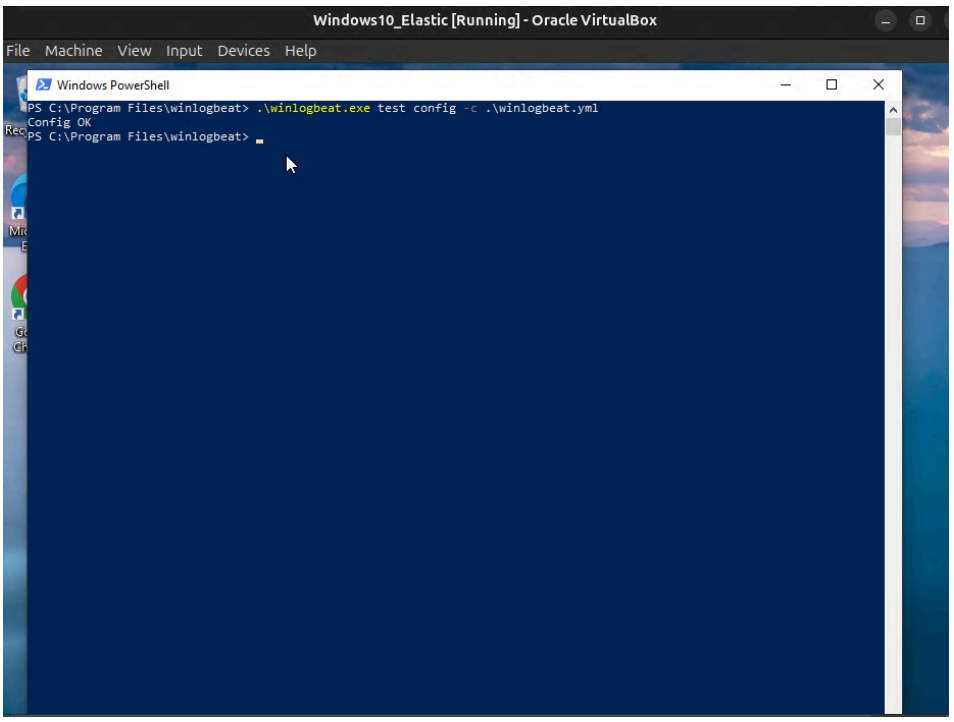
- Change "Array of hosts" to your Elastic IP.
- Comment the API key line and uncomment username/password, filling in the correct credentials.

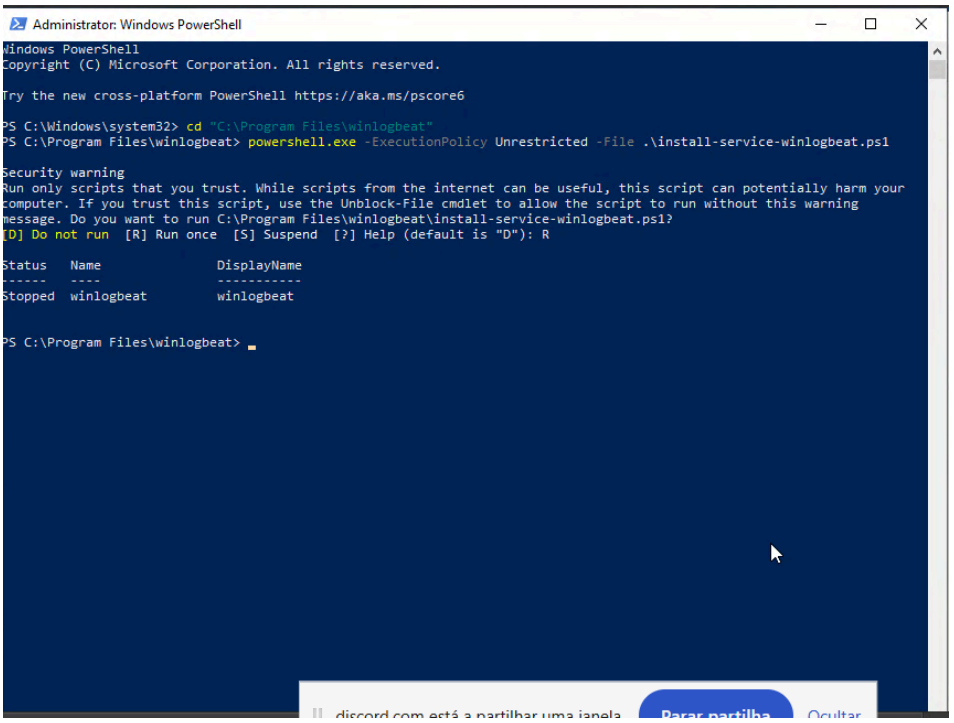


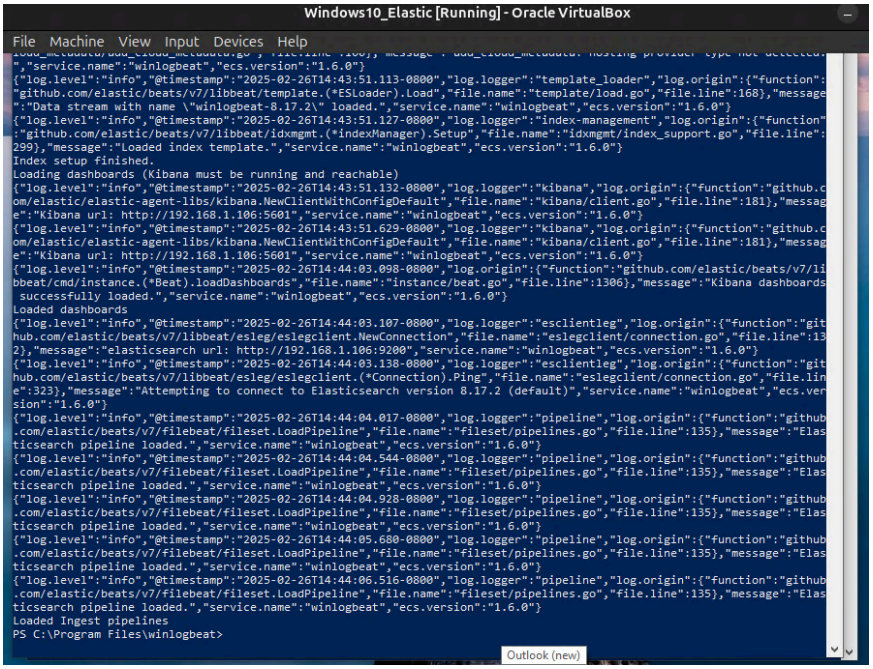
- Update Kibana hosts to your Elastic IP.

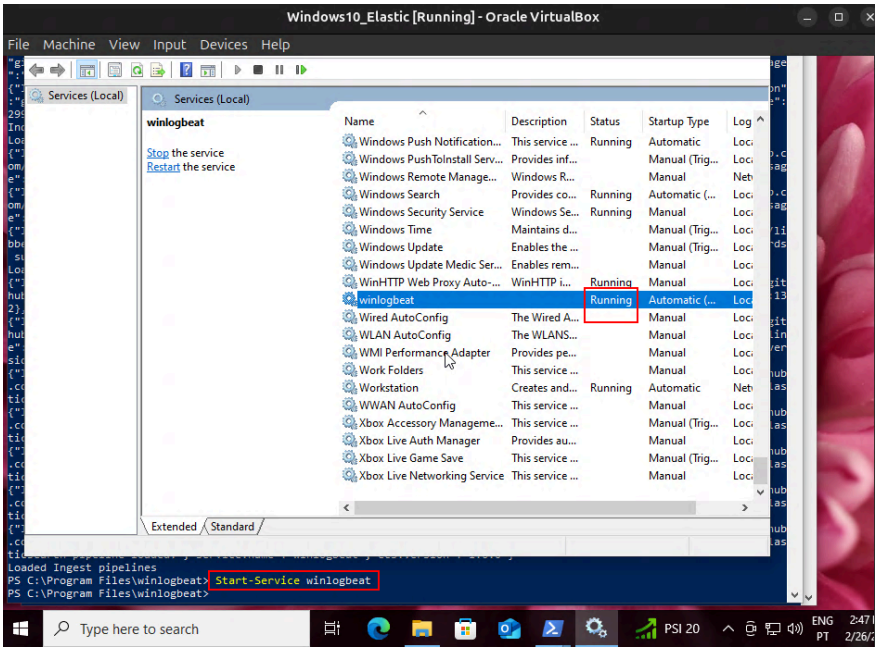


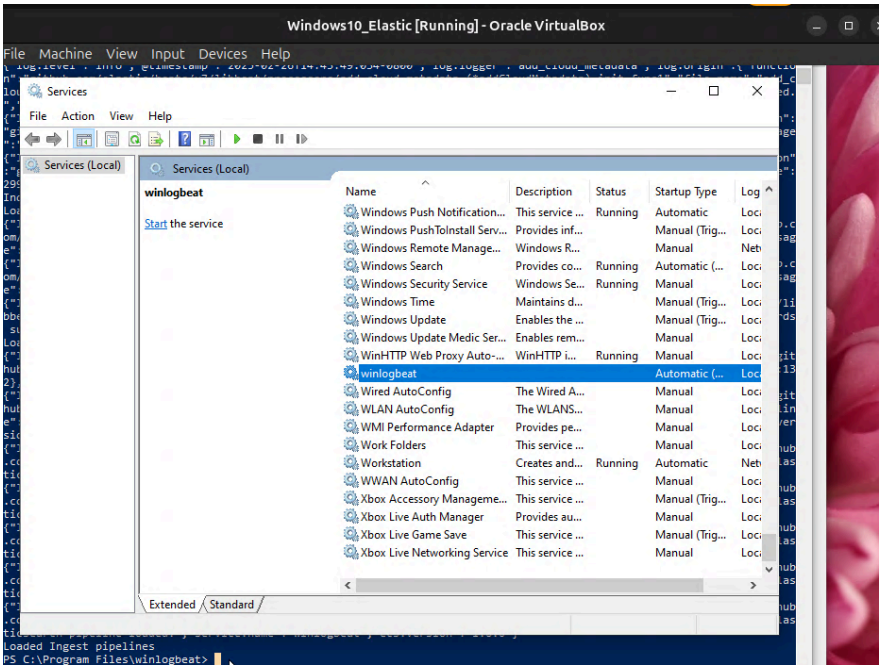
- Install Winlogbeat on the Windows 10 machine.


Windows10_Elastic [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Windows PowerShell
PS C:\Program Files\winlogbeat> .\winlogbeat.exe test config -c .\winlogbeat.yml
Config OK
PS C:\Program Files\winlogbeat>


Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.
Try the new cross-platform PowerShell https://aka.ms/pscore6
PS C:\Windows\system32> cd "C:\Program Files\winlogbeat"
PS C:\Program Files\winlogbeat> powershell.exe -ExecutionPolicy Unrestricted -File .\install-service-winlogbeat.ps1
Security warning
Run only scripts that you trust. While scripts from the internet can be useful, this script can potentially harm your computer. If you trust this script, use the Unblock-File cmdlet to allow the script to run without this warning message. Do you want to run C:\Program Files\winlogbeat\install-service-winlogbeat.ps1?
[D] Do not run [R] Run once [S] Suspend [?] Help (default is "D"): R
Status Name DisplayName
Stopped winlogbeat winlogbeat
PS C:\Program Files\winlogbeat>
discord.com está a partilhar uma janela
Parar partilha
Ocultar


Windows10_Elastic [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Outlook (new)


Windows10_Elastic [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Services (Local)
winlogbeat
Stop the service
Restart the service
Name
Description
Status
Startup Type
Windows Push Notification...
Windows PushToInstall Serv...
Windows Remote Manage...
Windows Search
Windows Security Service
Windows Time
Windows Update
Windows Update Medic Ser...
WinHTTP Web Proxy Auto-...
winlogbeat
Wired AutoConfig
WLAN AutoConfig
WMI Performance Adapter
Work Folders
Workstation
WWAN AutoConfig
Xbox Accessory Manageme...
Xbox Live Auth Manager
Xbox Live Game Save
Xbox Live Networking Service
Extended
Standard
Loaded Ingest pipelines
PS C:\Program Files\winlogbeat> Start-Service winlogbeat
PS C:\Program Files\winlogbeat>
Type here to search
PSI 20
ENG
PT



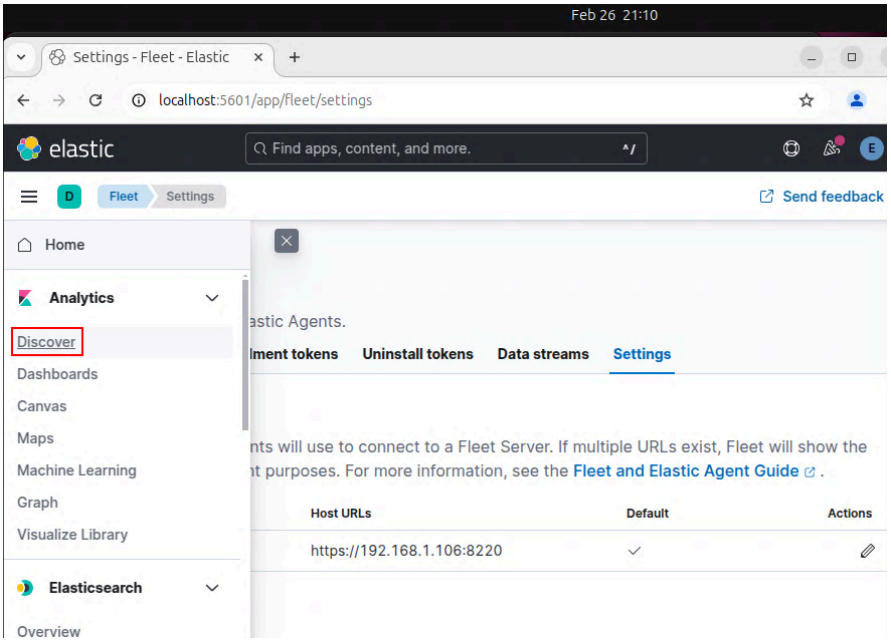
Part 2: Generate and Analyze Event Logs

1. Generate system activity

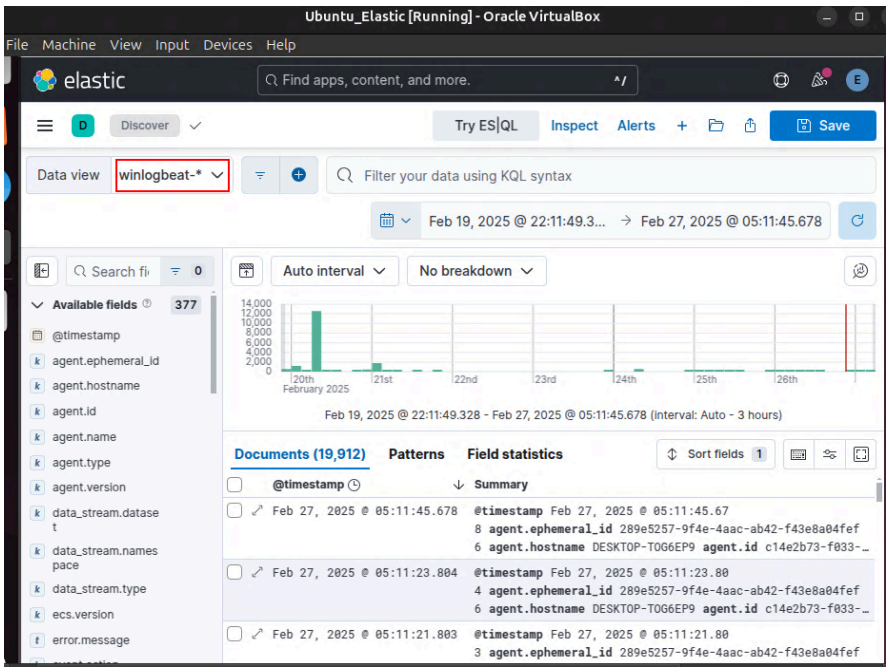
Perform several failed login attempts on the Windows 10 machine.

On Elastic, navigate to:

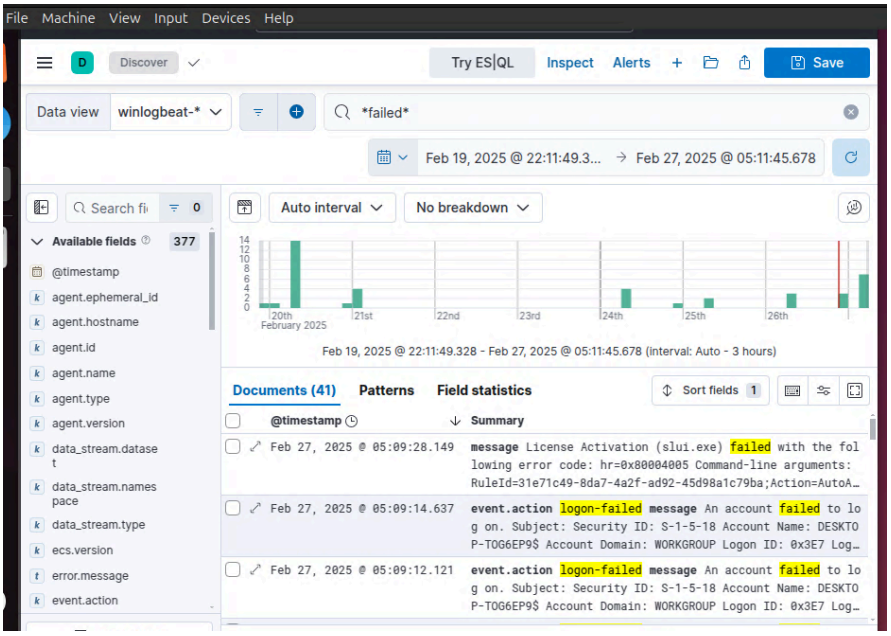
Analytics -> Discover



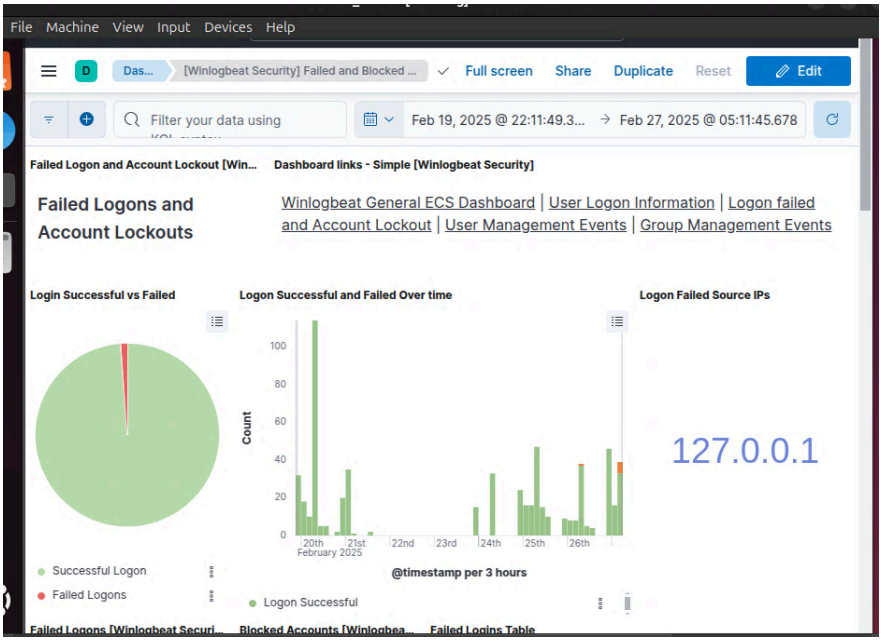
- Change Data Views to winlogbeat



- Check for failed login attempts.

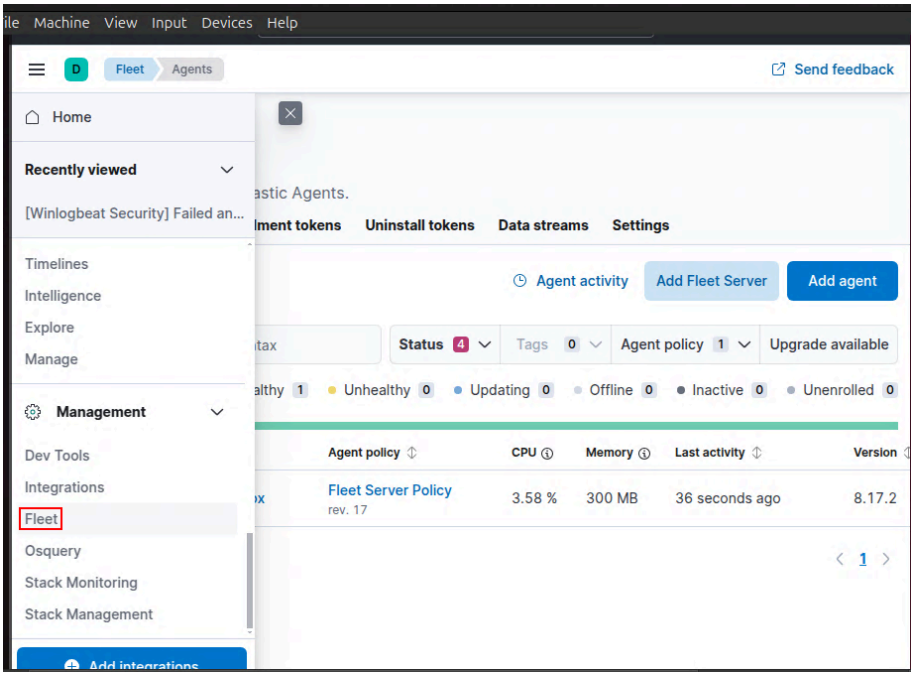


- If needed, refer to the [official Winlogbeat documentation] for event IDs
- For a more visual representation, check dashboards at: **Analytics -> Dashboard**

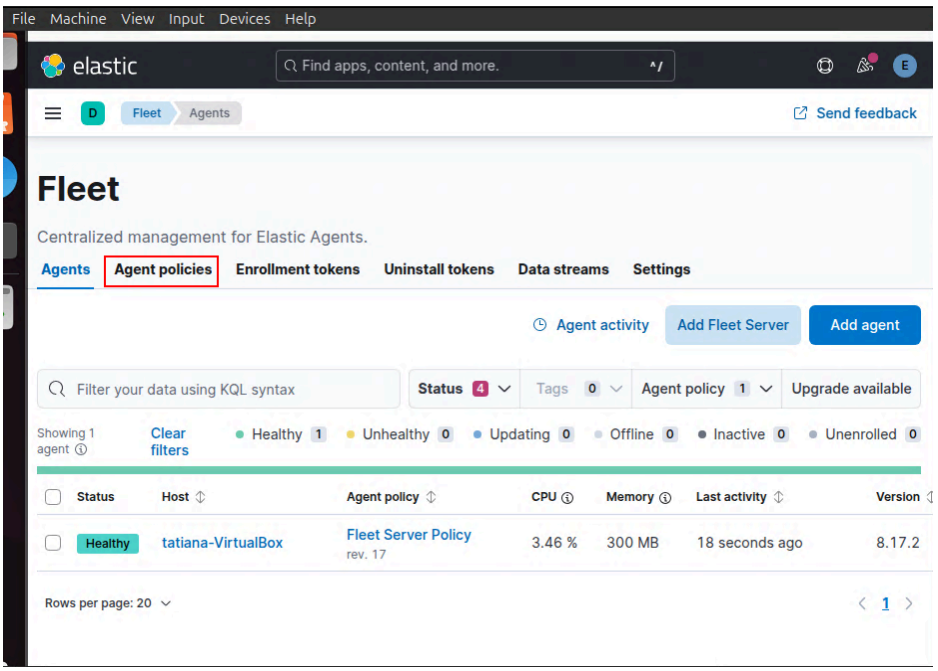


2. Install an agent on the Windows 10 machine

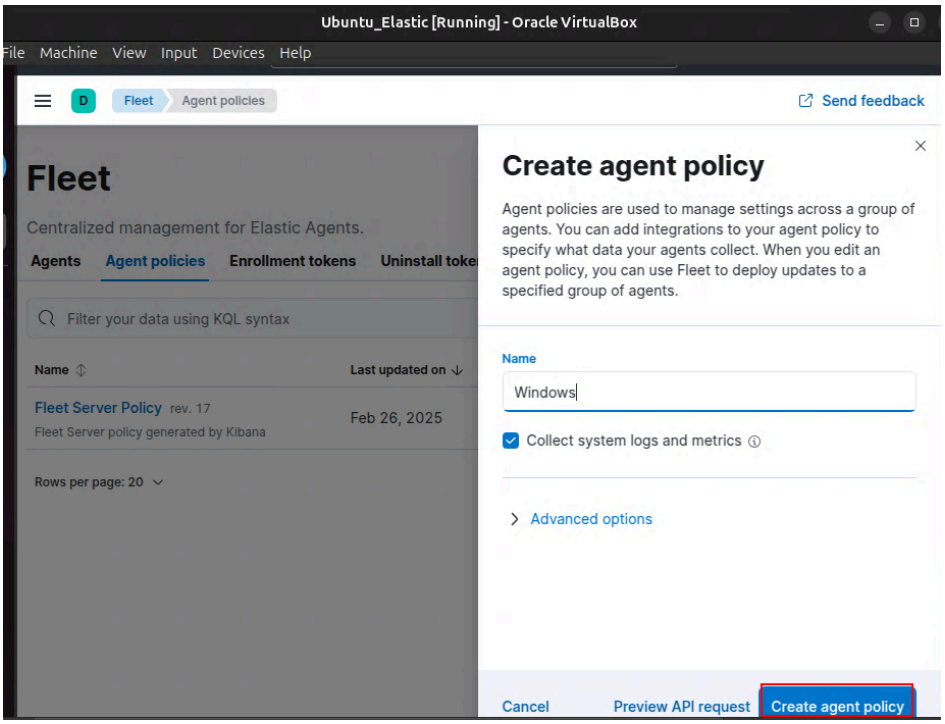
Go to "Agent policies" and create a new policy with 'System' and 'Elastic Defend'.



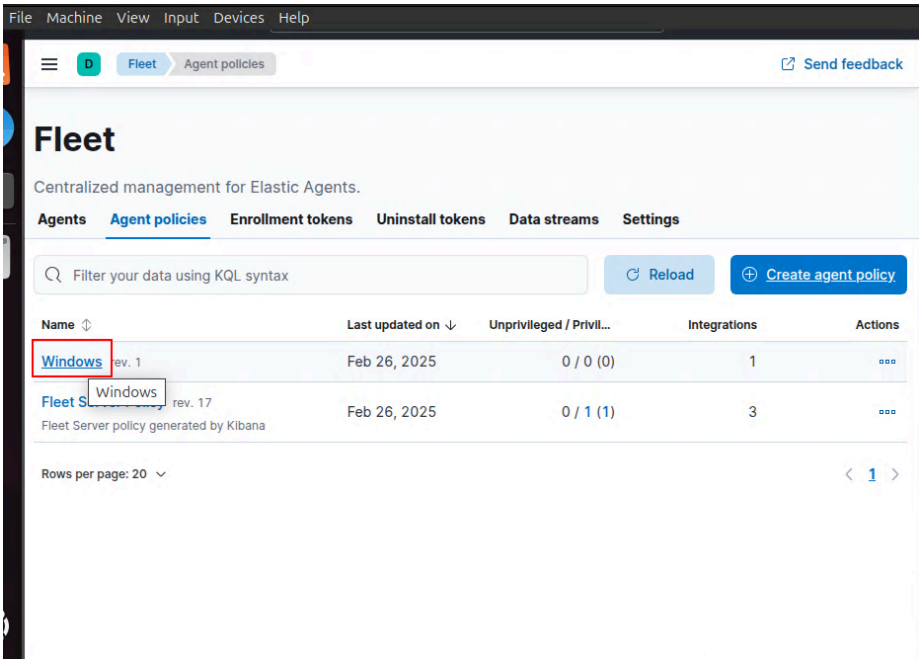
1. To add a new agent policy, we go to Fleet;



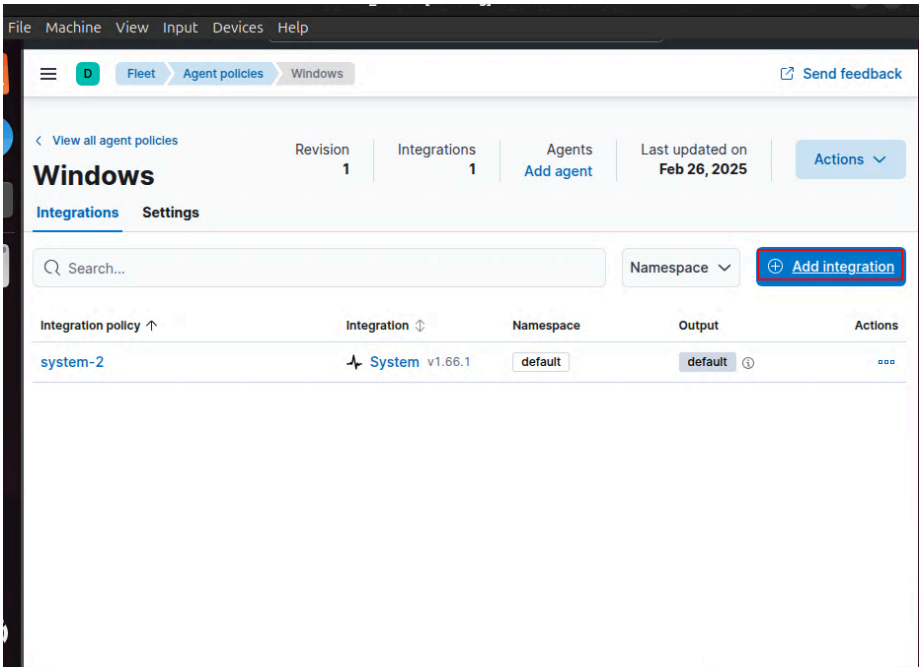
2. Select Agent Policies;



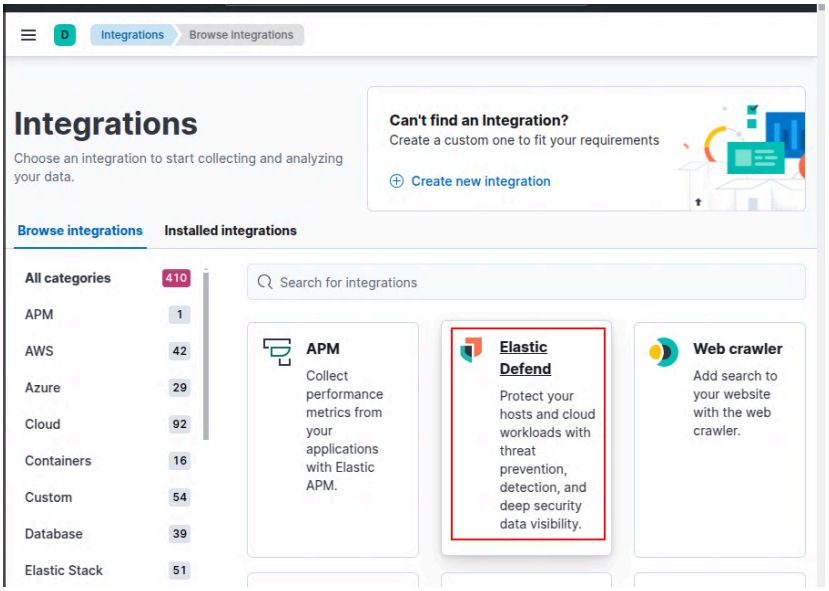
3. Give a name to the new policy and then create it;

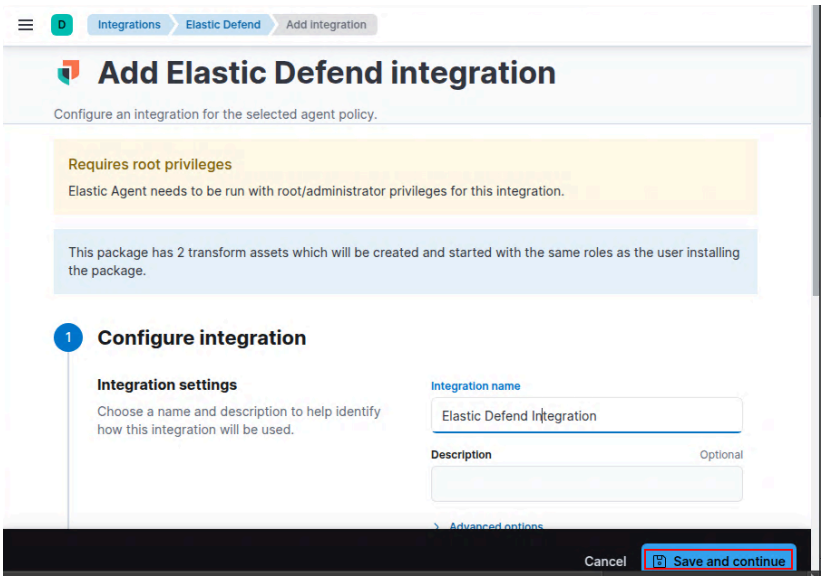


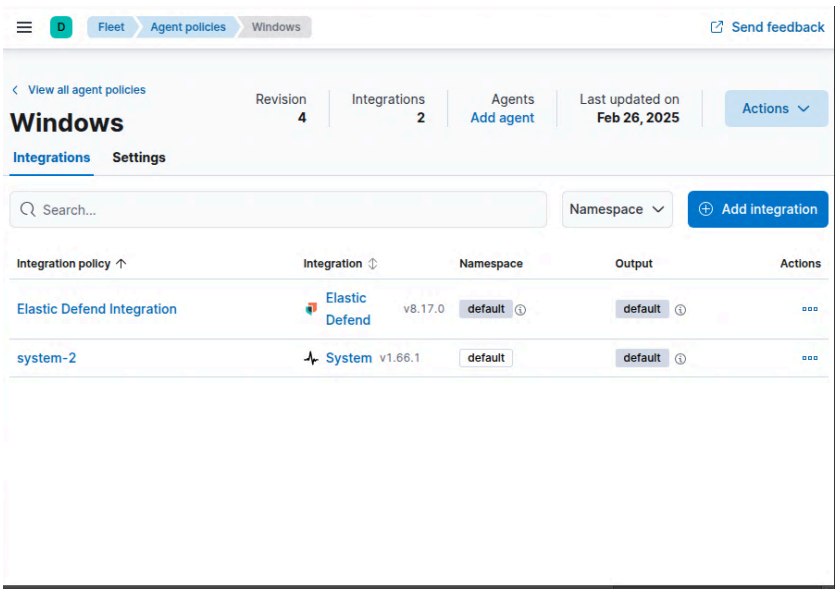
4. In order to add the integrations, we open the newly created policy;



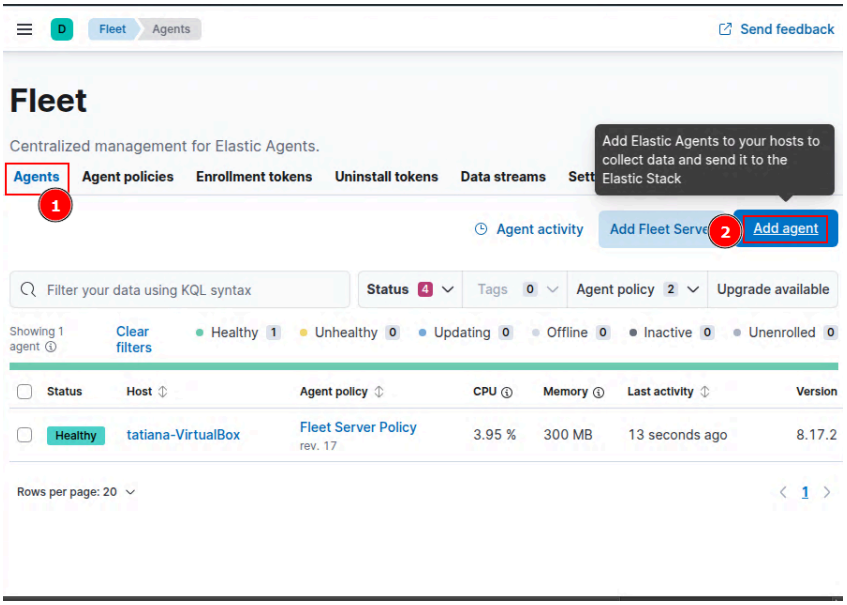
5. Select Add Integration


Integrations
Browse integrations
Integrations
Choose an integration to start collecting and analyzing your data.
Can't find an Integration?
Create a custom one to fit your requirements
Create new integration
Browse integrations
Installed integrations
All categories 410
APM 1
AWS 42
Azure 29
Cloud 92
Containers 16
Custom 54
Database 39
Elastic Stack 51
Search for integrations
APM
Collect performance metrics from your applications with Elastic APM.
Elastic Defend
Protect your hosts and cloud workloads with threat prevention, detection, and deep security data visibility.
Web crawler
Add search to your website with the web crawler.

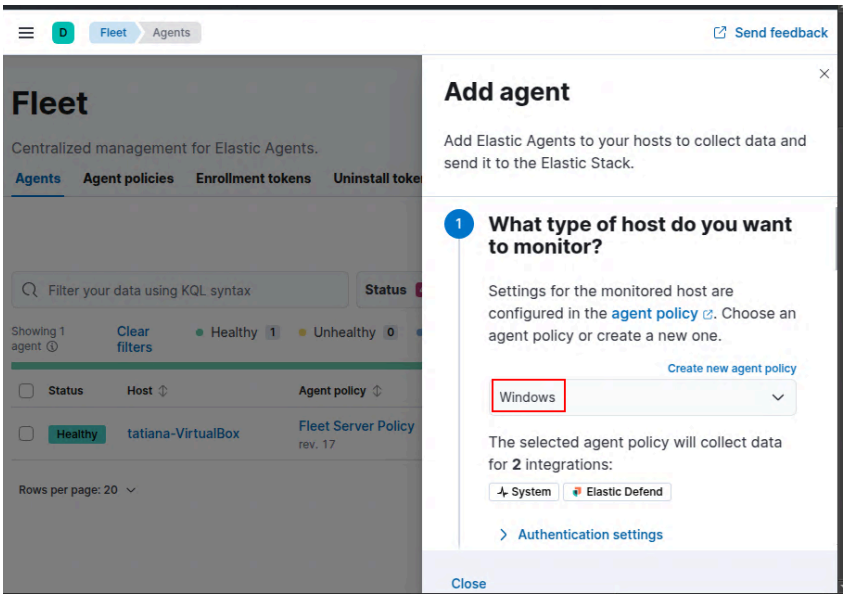

Integrations
Elastic Defend
Add integration
Add Elastic Defend integration
Configure an integration for the selected agent policy.
Requires root privileges
Elastic Agent needs to be run with root/administrator privileges for this integration.
This package has 2 transform assets which will be created and started with the same roles as the user installing the package.
1
Configure integration
Integration settings
Choose a name and description to help identify how this integration will be used.
Integration name
Elastic Defend Integration
Description
Optional
Advanced options
Cancel
Save and continue


Fleet
Agent policies
Windows
Send feedback
View all agent policies
Windows
Revision 4
Integrations 2
Agents Add agent
Last updated on Feb 26, 2025
Actions
Integrations
Settings
Search...
Namespace
Add integration
Integration policy
Integration
Namespace
Output
Actions
Elastic Defend Integration
Elastic Defend v8.17.0
default
default
system-2
System v1.66.1
default
default

6. Then select both integrations: System and Elastic Defend;



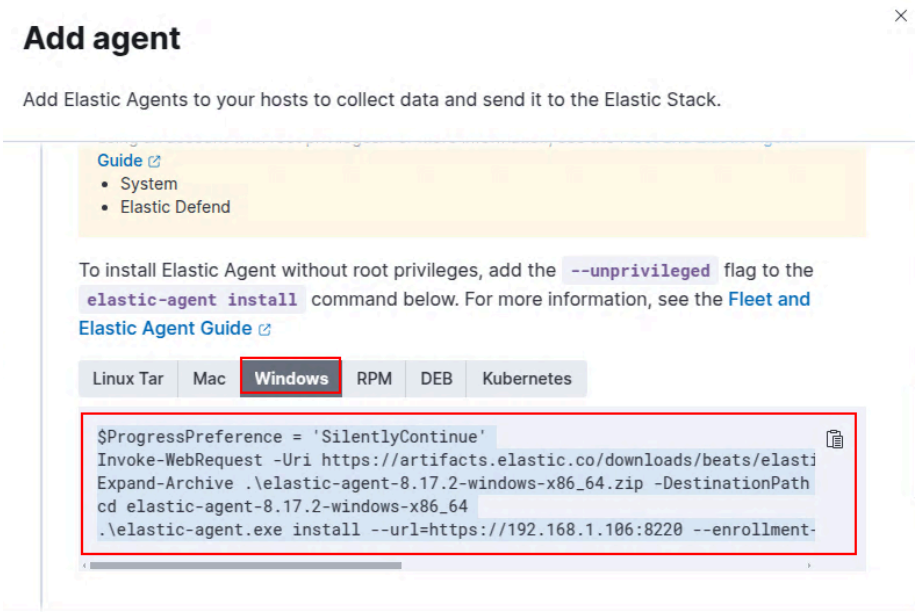
7. After adding the integrations, we need to add the agents;

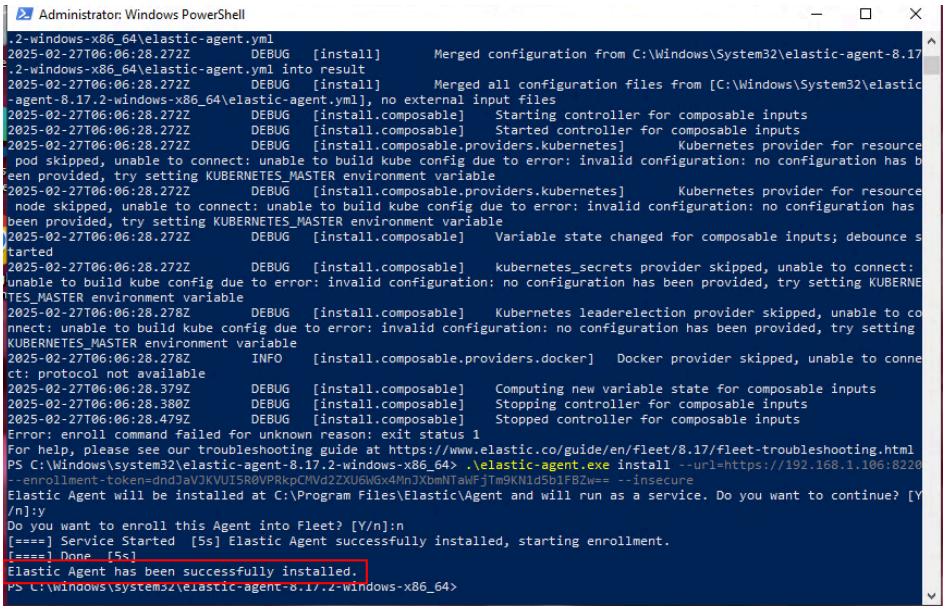


Go Fleet -> Add Agent -> Choose the newly created policy.

On the powershell script to enroll a new machine, add an "--insecure" at the end of the command.

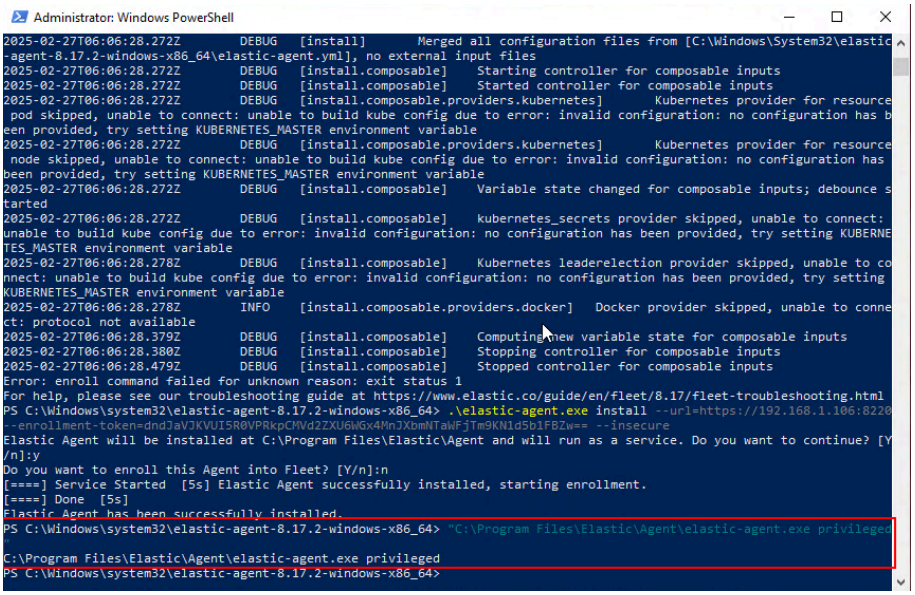
- The following command was run in PowerShell:





Make sure the agent is running with privileges:

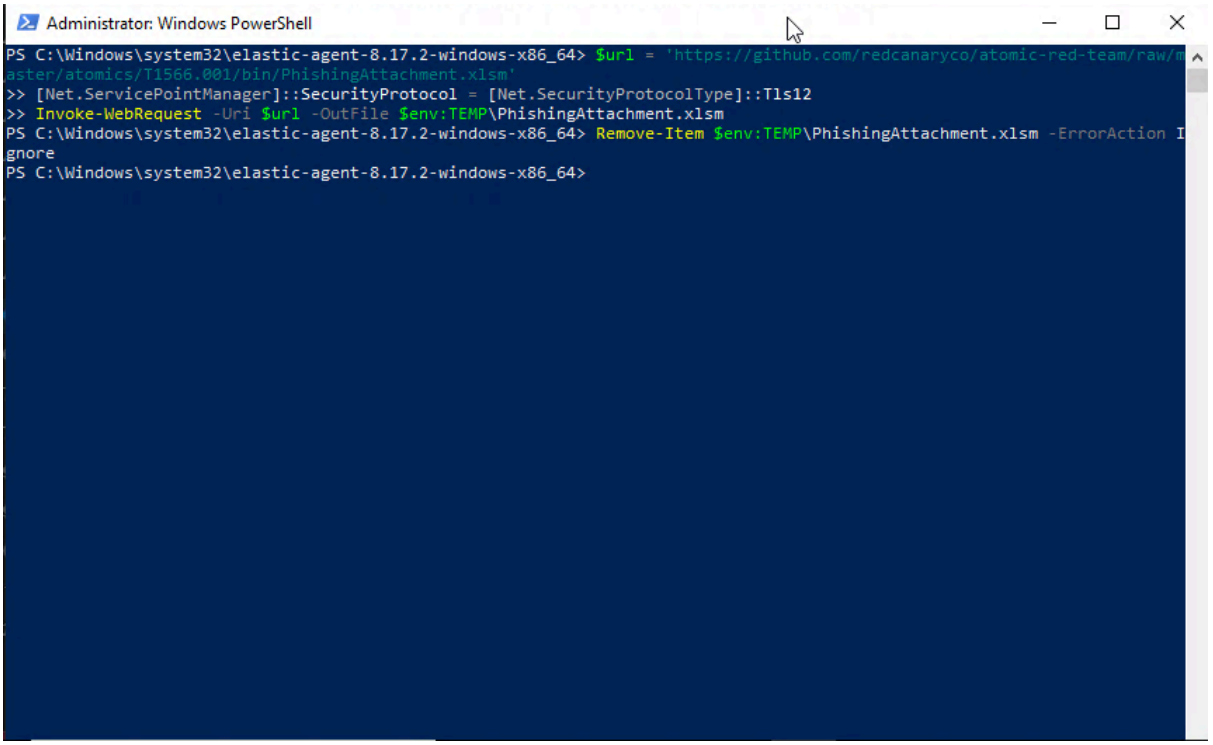
"C:Program Files\Elastic\Agent\elastic-agent.exe privileged".



3. Run tests

Run this atomic test:

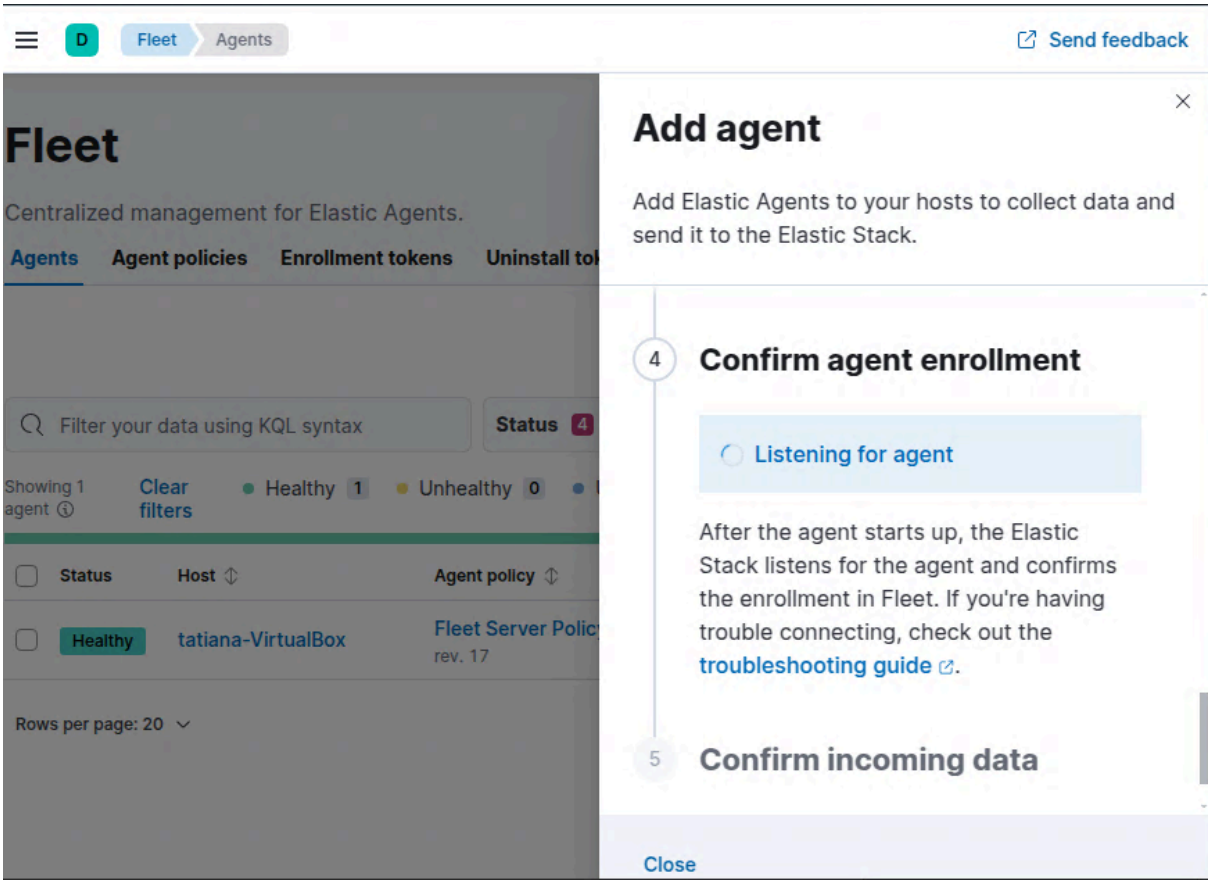
https://www.atomicredteam.io/atomic-red-team/atomics/T1566.001#atomic-test-1--- download-macro-enabled-phishing-attachment



4. Detect activities:

Go to "Observability" -> "Logs" and use file.name filter, to identify, creation of the

file, and the file deletion



Troubleshooting:

After all of the configurations were done in windows powershell, as shown in the previous printscreens, the agent does not start up.

Part 3: Documentation

To ensure GreenBloom maintains a strong security posture, your team must submit a detailed, step-by-step report documenting your entire configuration process. This documentation serves two key purposes:

Future Reference: Your team, and future analysts, will be able to replicate and refine this SIEM setup as GreenBloom's security needs evolve. A well-documented process ensures consistency in deployment and troubleshooting.

Company Records: As part of GreenBloom's cybersecurity services, detailed logs of

security implementations and testing procedures are essential for audits, compliance, and incident response planning.

Your report should include:

Setup Steps: A clear breakdown of how you configured Elastic SIEM, Winlogbeat, and other relevant components.

Testing Methodology: Details on how you executed Atomic Red Team tests, including the specific techniques used.

Detection and Analysis: Screenshots and explanations of security events detected in Kibana. **Challenges & Resolutions:** Any obstacles encountered and how you resolved them.

This documentation will be reviewed as part of your assessment and should be structured professionally, as if submitting it to GreenBloom's cybersecurity leadership.

By the end of this lab, you will have hands-on experience in SIEM deployment and testing, along with a valuable reference for future security operations. Now, let's secure GreenBloom!